UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/572,085	03/16/2006	Yong Man Shin	P/2803-66	9743

2352 7590 06/25/2009

OSTROLENK FABER GERB & SOFFEN
1180 AVENUE OF THE AMERICAS
NEW YORK, NY 100368403

EXAMINER	
BEYEN, ZEWDU A	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
06/25/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/572,085	SHIN ET AL.	
	Examiner	Art Unit	
	ZEWDU BEYEN	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-18, have been examined and are pending.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating

9. Claims 1-3, 5-9,11-16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Keshav (US 6754716) in view of Caves (US7490351).

Regarding claims 1, and 18 Keshav teaches determining at least a cut-off object device of which communication is needed to be cut-off, according to a set communication control rule(**col.5 lines 53-59, col.2 lines 40-46 disclose determining whether the requesting device is authorized to communicate with the target device by referring to the list authorized device address list)** ;

Though Keshav teaches sending ARP packet if the devices are authorized to communicate with each other, Keshav does not explicitly teach providing an address resolution protocol (ARP) packet in which a data link layer address is manipulated, to the cut-off object device, wherein the cut-off object device is controlled to transmit its data packets to manipulated abnormal addresses, and by doing so, communication by the cut-off object device is cut off.

However, Caves teaches ARP response spoofing by faking ARP response and forwarding traffic to the fake address **(col.2 lines 46-55 discloses faking ARP response traffic intended for a legitimate user will be forwarded to the malicious user, thus denying service to the sender and intended receiver)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav provide an address resolution protocol (ARP) packet in which a data link layer address is manipulated, to the cut-off object device, wherein the cut-off object device is controlled to transmit its data packets to manipulated abnormal addresses, and by doing so, communication by the cut-off object device is cut off, as suggested by Caves. This modification would benefit the system to efficiently block unwanted communication between devices.

Regarding claim 2, Keshav teaches transmitting an ARP packet including normal address information to a device which is in a communication cut-off state although the device is not an object of communication cut-off any more, such that the communication cut-off state is canceled**(col.2 lines 51-54 discloses if the device is authorized the ARP request is responded normally with a correct device address)**

Regarding claim 3, Keshav does not explicitly teach setting part or all of the data link layer

addresses of the cut-off object devices to the data link layer address of the communication control apparatus or a third data link layer address that is not of the cut-off object devices, such that communication between cut-off object devices is cut off.

However, Caves teaches responding ARP request with a fake address **(col.2 lines 46-55 discloses faking ARP response traffic intended for a legitimate user will be forwarded to the malicious user, thus denying service to the sender and intended receiver)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav setting part or all of the data link layer addresses of the cut-off object devices to the data link layer address of the communication control apparatus or a third data link layer address that is not of the cut-off object devices, such that communication between cut-off object devices is cut off, as suggested by Caves. This modification would benefit the system to efficiently block unwanted communication between devices.

Regarding claim 5, Keshav teaches collecting network layer addresses and data link layer addresses of network internal devices for which the communication control rule is set **(col.2 lines 29-36 discloses a list of the IP addresses of these authorized devices is stored in each of the network devices. The authorized IP address list is preferably loaded by each network device upon start up. The authorized IP address list updated periodically by a system administrator to reflect newly authorized devices, or to remove previously authorized devices)**

Regarding claim 6, Keshav teaches collecting address is performed by the address of an administration object device which is manually input by a network administrator, the

communication control apparatus transmits an ARP request packet and detects a network layer address and a data link layer address from an ARP reply packet transmitted by the administration object device in response to the ARP request packet**(col.2 lines 29-36 discloses a list of the IP addresses of these authorized devices is stored in each of the network devices. The authorized IP address list is preferably loaded by each network device upon start up. The authorized IP address list updated periodically by a system administrator to reflect newly authorized devices, or to remove previously authorized devices)**.

Regarding claim 7, Keshav teaches collecting network layer addresses and data link layer addresses existing in the network, by a communication control apparatus**(col.2 lines 29-36 discloses a list of the IP addresses of these authorized devices is stored in each of the network devices. The authorized IP address list is preferably loaded by each network device upon start up. The authorized IP address list updated periodically by a system administrator to reflect newly authorized devices, or to remove previously authorized devices)**; storing communication control rules, which are set to perform desired communication control for collected addresses by a network administrator, in a communication control rule database (DB) **(col.2 lines 29-36 discloses a list of the IP addresses of these authorized devices is stored in each of the network devices. The authorized IP address list is preferably loaded by each network device upon start up. The authorized IP address list updated periodically by a system administrator to reflect newly authorized devices, or to remove previously authorized devices)**; detecting an address resolution protocol (ARP) packet transmitted by a device in the network in order to communicate with another device in the network**(col.2 lines 37-48 discloses detecting an address resolution protocol (ARP) packet**

transmitted by a device in the network in order to communicate with another device) determining whether or not the detected ARP packet corresponds to a communication cut-off object, by referring to the communication control rule DB**(col.5 lines 53-59, col.2 lines 40-46 disclose determining whether the requesting device is authorized to communicate with the target device by referring to the list authorized device address list)**;

Though Keshav teaches sending ARP packet if the devices are authorized to communicate with each other, Keshav does not explicitly teach if the packet corresponds to the communication cutoff object, transmitting an ARP for communication cut-off, wherein communication between network internal devices can be selectively controlled when necessary.

However, Caves teaches responding ARP request with a fake address **(col.2 lines 46-55 discloses faking ARP response traffic intended for a legitimate user will be forwarded to the malicious user, thus denying service to the sender and intended receiver)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav setting part or all of the data link layer addresses of the cut-off object devices to the data link layer address of the communication control apparatus or a third data link layer address that is not of the cut-off object devices, such that communication between cut-off object devices is cut off, as suggested by Caves. This modification would benefit the system to efficiently block unwanted communication between devices.

Regarding claim 8, Keshav teaches collecting address is performed by the address of an administration object device which is manually input by a network administrator, the communication control apparatus transmits an ARP request packet and detects a network layer

address and a data link layer address from an ARP reply packet transmitted by the administration object device in response to the ARP request packet**(col.2 lines 29-36 discloses a list of the IP addresses of these authorized devices is stored in each of the network devices. The authorized IP address list is preferably loaded by each network device upon start up. The authorized IP address list updated periodically by a system administrator to reflect newly authorized devices, or to remove previously authorized devices)**.

Regarding claim 9, Keshav teaches the objects of setting the communication control rule include communication between network layer addresses, communication between data link layer addresses, and communication between a network layer address and a data link layer address**(fig.4 discloses two communicating devices with authorized request. Where the authorization involves the L3 (network layer address) and L2 (data link layer address) of the devices)**

Regarding claim 11, Keshav does not explicitly teach when a reception side address is an object of cut-off, a cut-off packet is transmitted to the `same addresses` as the reception protocol address.

However, Caves teaches responding ARP request with a fake address **(col.2 lines 46-55 discloses faking ARP response traffic intended for a legitimate user will be forwarded to the malicious user, thus denying service to the sender and intended receiver. Though, Caves does not explicitly teach cut-off packet is transmitted to the `same addresses` as the reception protocol address, it would have been obvious to one ordinary skilled in the art to use the same addresses as the reception protocol address when transmitting the replay ARP to control network flooding)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav when a reception side address is an object of cut-off, a cut-off packet is transmitted to the `same addresses` as the reception protocol address, as suggested by Caves. This modification would benefit the system to efficiently block unwanted communication between devices.

Regarding claim 12, Keshav does not explicitly teach when a transmission side address is an object of cut-off, a cut-off packet is transmitted to `all` protocol-data link layer addresses belonging to the same network as that of the transmission side protocol.

However, Caves teaches responding ARP request with a fake address **(col.2 lines 46-55 discloses faking ARP response traffic intended for a legitimate user will be forwarded to the malicious user, thus denying service to the sender and intended receiver. Though, Caves does not explicitly teach to transmit cut-off packet to `all` protocol-data link layer addresses belonging to the same network as that of the transmission side protocol, it would have been obvious to one ordinary skilled in the art to transmit cut-off packet to `all` protocol-data link layer addresses belonging to the same network as that of the transmission side protocol when transmitting the replay ARP to control network flooding)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav to transmit cut-off packet to `all` protocol-data link layer addresses belonging to the same network as that of the transmission side protocol, as suggested by Caves. This modification would benefit the system to efficiently block unwanted communication between devices.

Regarding claim 13, Keshav teaches if a network internal device transmits an ARP reply packet in response to the ARP request packet transmitted by the communication control apparatus, retrieving an relation rule by using a transmission side address included in the detected reply packet**(col.2 lines 37-48 discloses detecting an address resolution protocol (ARP) packet transmitted by a device in the network in order to communicate with another device. Further more, col.5 lines 53-59, col.2 lines 40-46 disclose determining whether the requesting device is authorized to communicate with the target device by referring to the list authorized device address list)**

Keshav does not explicitly teach if the retrieval result indicates that there is a cut-off rule for the transmission side address, transmitting a cut-off packet to all protocol-data link layer address DBs (DB-3) belonging to the same network as that of the transmission side protocol.

However, Caves teaches responding ARP request with a fake address **(col.2 lines 46-55 discloses faking ARP response traffic intended for a legitimate user will be forwarded to the malicious user, thus denying service to the sender and intended receiver. Though, Caves does not explicitly teach transmitting a cut-off packet to all protocol-data link layer address DBs (DB-3) belonging to the same network as that of the transmission side protocol, However; it would have been obvious to one ordinary skilled in the art to transmitting a cut-off packet to all protocol-data link layer address DBs (DB-3) belonging to the same network as that of the transmission side protocol when transmitting the replay ARP to control network flooding)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav transmitting a cut-off packet to all protocol-

data link layer address DBs (DB-3) belonging to the same network as that of the transmission side, as suggested by Caves. This modification would benefit the system to efficiently block unwanted communication between devices.

Regarding claim 14, Keshav teaches for a device which is in a communication cut-off state although the device is not an object of communication cut-off any more with detection of a network layer packet, transmitting an ARP packet for canceling the communication cut-off state**(col.2 lines 51-54 discloses if the device is authorized the ARP request is responded normally with a correct device address. Further more, col.2 lines 29-36 discloses authorized IP address list updated periodically by a system administrator to reflect newly authorized devices, or to remove previously authorized devices)**.

Regarding claim 16, Keshav teaches if a reception side data link layer address is a cut-off address and there is a packet forwarding rule for the address, forwarding the received protocol layer packet with having the destination address of the received protocol layer packet as a normal data link layer address**(col.2 lines 51-54 discloses if the device is authorized the ARP request is responded normally with a correct device address)**.

Regarding claim 15, Keshav teaches by referring to the communication control rule DB at regular time interval, transmitting an ARP request packet for communication cut-off/canceling communication cut-off according to a communication control rule registered in the DB**(col.2 lines 37-48 discloses detecting an address resolution protocol (ARP) packet transmitted by a device in the network in order to communicate with another device. Further more, col.5 lines 53-59, col.2 lines 40-46 disclose determining whether the requesting device is**

authorized to communicate with the target device by referring to the list authorized device address list. Though, the device communication rule (authorized list) is not stored in a database , it would have been obvious to one ordinarily skilled in the art to store the communication rule in a database as a design choice).

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Keshav (US 6754716) in view of Caves (US7490351), and further in view of Wiegand to **(US 20070055752)**

Regarding claim 10, Keshav does not explicitly teach the objects of setting the communication control rule further include communication between network layer address and network layer address groups, communication between data link layer address and data link layer address groups, communication between network layer addresses and data link layer address groups, communication between data link layer addresses and network layer address groups, and communication between network layer address groups and data link layer address groups

However, Wiegand teaches the objects of setting the communication control rule further include communication between network layer address and network layer address groups, communication between data link layer address and data link layer address groups, communication between network layer addresses and data link layer address groups, communication between data link layer addresses and network layer address groups, and communication between network layer address groups and data link layer address groups**([0004] discloses enabling compliance of a communication device with the policies of a destination network, a communication device configured to connect to a compliance network; the**

compliance network configured to check whether the communication device is sufficiently in compliance with at least one predetermined policy of a destination network and to not allow the communication device to connect with the destination network if the communication device is not sufficiently in compliance with the at least one predetermined policy. Further more, [0005] discloses means for selecting a connection between the communication device and a destination network or between the communication device and a compliance network exclusive of the destination network; and means for establishing the selected connection; wherein the means for selecting is configured to select the connection with the compliance network exclusive of the destination network when a likelihood that the communication device is not in sufficient compliance with at least one predetermined policy of the destination network exceeds a predetermined level. Though, Wiegand does not explicitly teach setting the communication control rule using different network addresses, it is inherent to the system to be able to implement the above policy)

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav setting setting the communication control rule further include communication between network layer address and network layer address groups, communication between data link layer address and data link layer address groups, communication between network layer addresses and data link layer address groups, communication between data link layer addresses and network layer address groups, and communication between network layer address groups and data link layer address groups, as suggested by Wiegand. This modification would benefit the system to efficiently block unwanted communication between devices.

Claims 4 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Keshav (US 6754716) in view of Caves (US7490351), and further in view of Davis to (US7496095)

Regarding claims 4, and 17 Keshav does not explicitly teach if there is collision between the Internet protocol (IP) address of a device newly connected to the predetermined network and the IP addresses of existing devices, transferring a correct IP address to the existing devices in a unicast method such that the collision of the IP address is prevented

However, Davis teaches transmission of a unicast ARP replay with IP address **(col.10 lines 63-66 discloses sending a unicast ARP response with the network IP address)**

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to enable the system of Keshav if there is collision between the Internet protocol (IP) address of a device newly connected to the predetermined network and the IP addresses of existing devices, transferring a correct IP address to the existing devices in a unicast method such that the collision of the IP address is prevented, as suggested by Davis. This modification would benefit the system to securely transmit the network address to the intended device.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ZEWDU BEYEN whose telephone number is (571)270-7157. The examiner can normally be reached on Monday thru Friday, 9:30 AM to 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on 1-571-272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Z. B./

Examiner, Art Unit 2416

/Huy D. Vu/

Supervisory Patent Examiner, Art Unit 2416